(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(11) **DE 3507744 A1**

(51) Int. Cl. 4:
G06F 12/14

(21) Aktenzeichen: P 35 07 744.1
(22) Anmeldetag: 5. 3. 85
(43) Offenlegungstag: 11. 9. 86

DE 3507744 A1

(71) Anmelder:
Neumann, Hans-Günter, Dr., 5047 Wesseling, DE

(72) Erfinder:
Neumann, Karl-Joachim, 5047 Wesseling, DE

(54) Verfahren zum Schutz von Datenbanken und/oder Rechenanlagen der elektronischen Datenverarbeitung und/oder Datentechnik vor dem Zugriff Unberechtigter

Nach dem Verfahren wird der direkte Zugang zu einer Datenbank und oder Rechenanlage durch das Zwischenschalten einer Vorrichtung (Datenvermittlung und/oder Datentransferstation) fernmeldetechnisch abgekoppelt.
Die Datenvermittlung und/oder Datentransferstation wikkelt Eingänge und Abfragen von Daten zu und aus der Datenbank und/oder Rechenanlage vorzugsweise mechanisch (und automatisch) ab.
Unberechtigte haben somit nur Zugang zur Datenvermittlung und/oder Datentransferstation, nie aber zu Daten der Datenbank und/oder Rechenanlage selbst.
Die Zwischenschaltung der Vorrichtung verzögert den Datentransfer um höchstens 1-2 Minuten, nicht aber die Übertragungsraten.

DE 3507744 A1

BNSDOCID: <DE___3507744A1 | >

PATENT - ANSPRÜCHE

3507744

1. Verfahren zum Schutz von Datenbanken und/oder Rechenanlagen in der elektronischen Datenverarbeitung und/oder Datentechnik vor dem Zugriff Unberechtigter,

dadurch gekennzeichnet, daß

die elektronische Datenverarbeitungsanlage (EDV) und/oder Datenbank und/oder Rechenanlage räumlich und/oder elektrisch und/oder fernmeldetechnisch und/oder datenleitungsmäßig von einer Datenvermittlung und/oder Datentransferstation abgetrennt ist.

2. nach Anspruch 1. eine Datenvermittlung und/oder Datentransferstation besteht, die den Außenverkehr und/oder innerbetrieblichen Verkehr mit der Datenbank und/oder Rechenanlage selbständig und unabhängig von der Datenbank und/oder Rechenanlage abwickelt.

3. nach den Ansprüchen 1. und 2. die Datenvermittlung und/oder Datentransferstation vorzugsweise jeden Datenverkehr von und/oder zur Datenbank und/oder Rechenanlage auf eine Berechtigung, mit der Datenbank und/oder Rechenanlage zu kommunizieren, überprüft.

4. nach den Ansprüchen 1. bis 3. die Überprüfung eines Datentransfers vorzugsweise darin besteht, daß vor jedem Datentransfer eine Anmeldung des Anfragenden zu erfolgen hat, die sich die Datenvermittlung und/oder Datentransferstation, vorzugsweise nach Abtrennen der Rufverbindung, durch Rückruf vom Anfragenden bestätigen läßt.

5. die Anmeldung nach Anspruch 4. Angaben über die Art und Menge der angefragten und/oder der einzugebenden Daten enthält.

6. vorzugsweise nach den Daten der Anmeldung nach Anspruch 5. eine Überprüfung für die Berechtigung der zu versendenden und/oder zu empfangenden Daten erfolgt.

7. nach den Ansprüchen 3. bis 6. nach festgestellter und bestätigter Berechtigung einzugebende Daten von der Datenvermittlung und/oder Datentransferstation vom Absender abgerufen und auf einem Datenträger vorzugsweise in der Datenvermittlung und/oder Datentransferstation gespeichert werden.

8. nach Anspruch 7. der Datenträger mit den empfangenen und gespeicherten Daten vorzugsweise mechanisch an die Datenbank und/oder Rechenanlage übergeben wird und dort erst in die Datenbank und/oder Rechenanlage eingelesen wird.

9. nach festgestellter Berechtigung nach den Ansprüchen 3. bis 6. auszugebende und/oder abzusendende Daten bei der Datenbank und/oder Rechenanlage, vorzugsweise entsprechend der Anmeldung bestellt werden.

-/2

10. die nach Anspruch 9. bestellten Daten in der Datenbank und/oder Rechenanlage auf einen, vorzugsweise getrennt laufenden Datenträger eingelesen und gespeichert werden und dieser Datenträger vorzugsweise mechanisch an die Datenvermittlung und/oder Datentransferstation überstellt wird.

11. die nach Anspruch 10. überstellten Daten von der Datenvermittlung und/oder Datentransferstation, vorzugsweise nach vorheriger Überprüfung einer korrekten Verbindung, dem Anfragenden und/oder Besteller übersendet werden.

12. nach den Ansprüchen 9. bis 11. der Anfragende und/oder Besteller und/oder Empfänger der Daten, vorzugsweise nach Trennen der bestehenden Verbindung, den Empfang der Daten bestätigt.

13. nach den Ansprüchen 1. bis 12. die Datenvermittlung nur die Überprüfung der Berechtigungen durchführt und die Datentransferstation räumlich und/oder elektrisch und/oder fernmeldetechnisch und/oder datenleitungsmäßig von der Datenvermittlung getrennt ist.

14. nach den Ansprüchen 1. bist 13. die Datenvermittlung und/oder Datentransferstation aus einer selbständigen Einheit besteht, die eine Rechenanlage und oder Rechner sein kann, die alle Funktionen vorzugsweise vollautomatisch und/oder programmgesteuert ausführt, ~~mit Ausnahme des mechanischen Transports der Datenträger~~.

Anmelder: Dr. Hans-Günter Neumann, Elsterweg 5, 5047 WESSELING
Erfinder: Karl-Joachim Neumann, Elsterweg 5, 5047 WESSELING

GEGENSTAND UND BEZEICHNUNG:

Verfahren zum Schutz von Datenbanken und/oder Rechenanlagen der elektronischen Datenverarbeitung und/oder Datentechnik vor dem Zugriff Unberechtigter.

Die vorgelegte Erfindung betrifft ein Verfahren zum Schutz von Datenbanken und/oder Rechenanlagen der elektronischen Datenverarbeitung und/oder Datentechnik vor dem Zugriff Unberechtigter.

Nach dem Stand der Technik wird es als unmöglich angesehen, Datenbanken und/oder Rechenanlagen vor dem Zugriff Unberechtigter (Hacker) zu schützen.

Diskussionen, Berichte und Untersuchungen in Medien und der Fachliteratur beklagen immer häufiger, daß es Hackern per Datenfernübertragung (DÜF) gelingt, in noch so gut durch Kodes gesicherte Datenbanken und Rechenanlagen Eingang zu finden, dort Daten abzurufen oder gar zu verändern.

Die Ursache für diese Möglichkeiten liegt in der Technologie der elektronischen Datenverarbeitung begründet.

Ein Kodewort (Password) und sei es noch so verschlüsselt, muß irgendwo im ROM, RAM oder auf einem Datenträger der Rechenanlage gespeichert sein, um berechtigten Benutzern den Eingang in die Anlage und den Zugang zu Daten zu ermöglichen.

Gelingt es nun einem unberechtigten Benutzer (Hacker) bis in den Eingang (Input) einer Datenbank oder Rechenanlage vorzudringen, was nach Ansicht und Erfahrung von Fachleuten keinerlei Schwierigkeiten bereitet, ist es nur noch eine Frage der Zeit und des Aufwandes, wann ein Hacker die Kodes findet und damit Zugang zu den Daten.

Mit Kenntnis des Kodes ist es nunmehr dem unberechtigten Benutzer möglich, lange Zeit unentdeckt Daten abzurufen, zu verändern oder sogar zu löschen. Die hierdurch anzurichtenden Schäden können erheblich sein. Vor allem machen sie alle Versuche eines wirkungsvollen Datenschutzes persönlicher oder geheimer Daten zunichte.

Ähnliche Probleme treten auf, wenn Programmierer oder EDV-Techniker den Arbeitsplatz wechseln oder als Bedienungspersonal einer Datenbank oder Rechenanlage ausscheiden.

Sie kennen die Kodes und die Architektur der Datenbank oder der Rechenanlage oder können gar vor ihrem Ausscheiden eine Hintertür einprogrammieren,über die sie jederzeit Eingang in die Anlage finden können.

-/2

Das zum Patent angemeldete Verfahren geht davon aus, daß ein wirksamer Kode-Schutz nicht möglich ist und in Zukunft auch nicht möglich sein wird.

Das erfindungsgemäße Verfahren besteht darin, daß zwischen die Datenbank und/oder Rechenanlage eine Datenvermittlung geschaltet wird.

Diese Datenvermittlung funktioniert ähnlich einer Telefonvermittlung oder Telefonzentrale, nur besitzt diese Datenvermittlung zur Datenbank und/oder Rechenanlage keine Datenleitung oder irgend eine andere fernmeldetechnische Verbindung.

Zur Beschreibung der Datenvermittlung und deren Funktion soll von zwei Möglichkeiten ausgegangen werden:

1. Einzugebende Daten:

   Die Datenvermittlung übernimmt automatisch den Anruf eines Benutzers der Datenbank und/oder Rechenanlage, der die Absicht hat, Daten einzugeben.

   Der Anruf wird registriert (Datum, Uhrzeit, Teilnehmernummer) und danach die Leitungsverbindung zum Anrufer unterbrochen.

   In einem Benutzerkatalog der Datenvermittlung wird nun überprüft, ob es sich um einen berechtigten Benutzer handelt.

   Nach positivem Ergebnis dieser Kontrolle und Überprüfung stellt die Datenvermittlung vorzugsweise automatisch eine erneute Verbindung mit dem Anrufer her und übernimmt nun alle eingehenden Daten auf einen Datenträger (z.B. eine Wechselplatte).

   Je nach vorher vereinbartem Vorrang wird nach beendetem Datentransfer oder in vorgegebenen Zeitabständen der Datenträger vorzugsweise mechanisch in die Datenbank und/oder Rechenanlage überstellt und dort von einem Lesegerät die Daten von dem Datenträger in die Datenbank und/oder Rechenanlage eingelesen.

2. Auszugebende Daten oder Programme:

   Die Datenvermittlung übernimmt vorzugsweise automatisch den Anruf für eine Datenanfrage und behandelt diese Anfrage als Anmeldung für einen Abrufauftrag.

   Die Anmeldung sollte Datum, Uhrzeit, Benutzernummer und Art und Umfang der zu übermittelnden Daten enthalten.

   Nach Trennung der Leitungsverbindung wird die Anmeldung im Katalog der Datenvermittlung auf Berechtigung überprüft.

   Handelt es sich bei dem Anrufer um einen unberechtigten Benutzer oder ist der Anrufer Benutzer, jedoch für den Empfang dieser Daten unberechtigt, endet hier die Tätigkeit der Datenvermittlung.

-/3

Handelt es sich bei der Anmeldung für die zu transferierenden Daten um die eines berechtigten Benutzers, stellt die Datenvermittlung vorzugsweise automatisch durch Rückruf fest, ob diese Daten bestellt worden sind.

Wird die Bestellung der Daten von dem brechtigten Benutzer bestätigt, wird die Verbindung zum Benutzer wieder getrennt.

Vorzugsweise mechanisch (z.B. durch Rohrpost) wird die Datenbestellung nunmehr an die Datenbank und/oder Rechenanlage übermittelt, die dann die gewünschten Daten auf einen Datenträger transferiert, der dann vorzugsweise mechanisch der Datenvermittlung zugestellt wird.

Die Datenvermittlung stellt nunmehr erneut eine Verbindung mit dem berechtigten Benutzer und Anmelder her und überträgt nach Bestätigung der korrekten Verbindung die Daten an den berechtigten Benutzer.

Zur Erhöhung der Sicherheit kann bei wichtigen Daten noch eine zusätzliche Transferstation eingerichtet werden, die den Transfer unabhängig und ohne Leitungsverbindung zur Datenvermittlung und der Datenbank und/oder Rechenanlage auf Bestellung der Datenvermittlung abwickelt.

Zwischen den einzelnen Stationen bestehen zu keiner Zeit irgendwelche Leitungsverbindungen. Auf diese Weise kann ein Unberechtigter niemals bis zur Datenbank und/oder Rechenanlage vordringen.

Datenvermittlung und/oder Transferstation sind selbständige Rechenanlagen und/oder Rechner, die nur die Abwicklung des Datentransfers vollautomatisch abwickeln.

Der Datentransport von diesen Einrichtungen zur eigentlichen Datenbank und/oder Rechenanlage und zurück erfolgt vorzugsweise rein mechanisch (z.B. durch Rohrpost, Aufzug usw.).

Für die Datenvermittlung und/oder Datentransferstation lassen sich spezielle Rechner oder Rechenanlagen verwenden, die mit geeigneten Software-Programmen und Interfaces auszustatten sind.

Bei Einsatz dieser Rechenanlagen als Zwischenstationen werden die Zugriffszeiten zu Datenbanken und/oder Rechenanlagen nur unwesentlich erhöht, dafür aber ein unberechtigter Zugriff vollständig ausgeschlossen, da zur eigentlichen Datenbank und/oder Rechenanlage überhaupt keine Verbindung besteht.